申請日期	89 年 3 月 10 日
案號	89104427
類別	G06F 15/00

（以上各欄由本局填註）

A4
C4

公告本

470889

發明 新型 專利說明書

一、發明新型名稱	中文	電腦系統及內容保護方法
	英文	
二、發明創作人	姓名	(1) 石橋泰博 (2) 上林達 (3) 田村正文
	國籍	(1) 日本 (2) 日本 (3) 日本
	住、居所	(1) 日本國東京都青梅市新町九－四－一 魯美耶魯新町一－三一三 (2) 日本國神奈川縣茅ケ崎市本宿町三－一八－一〇八 (3) 日本國東京都調布市調布ヶ丘一－一八－七六－七〇六
三、申請人	姓名（名稱）	(1) 東芝股份有限公司 株式会社東芝
	國籍	(1) 日本
	住、居所（事務所）	(1) 日本國神奈川縣川崎市幸區堀川町七二番地
	代表人姓名	(1) 西室泰三

裝 訂 線

A5
B5

四、中文發明摘要（發明之名稱：電腦系統及內容保護方法）

本發明係關於電腦系統及被適用於該電腦系統之內容保護方法。其手段爲：安全管理者（１１２）在使用具有媒體ＩＤ之記錄媒體（１１６、１１７）之情形，於每個記錄內容之記錄媒體使用該媒體ＩＤ進行內容之加密／解碼之管理。另一方面，在使用不具有媒體ＩＤ之ＨＤＤ（１１５）之情形，安全管理者（１１２）透過ＢＩＯＳ取得電腦系統之固有的裝置ＩＤ，使用該裝置ＩＤ管理記錄在ＨＤＤ之內容之加密／解碼。裝置ＩＤ被記憶在電腦系統內之安全的領域。藉由此，即使在硬碟之類的開放式記錄媒體中記錄內容之情形，可以保護該內容被不正當使用，能一併謀求數位內容之利用與保護。

英文發明摘要（發明之名稱：）

（請先閱讀背面之注意事項再填寫本頁各欄）

裝 訂 線

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
IPC分類：	

本案已向：

國（地區）	申請專利，申請日期：	案號：	，□有　□無主張優先權
日本	1999 年 4 月 28 日	11-122001	☑有主張優先權

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

五、發明說明（1）

發明背景

本發明係關於電腦系統及被適用於該電腦系統之內容保護方法。

近年來伴隨電腦技術之發達，各式各樣之對應多媒體之個人電腦正被開發著。此種個人電腦可以通過網路下載影像資料或音樂資料等之數位內容使用。

這些數位內容藉由ＭＰＥＧ２、ＭＰ３之所謂的數位編碼技術之採用，可以不降低品質下載。因此，最近由著作權保護之觀點而言，保護此種數位內容被不正當使用之技術必要性乃隨之產生。

但是，個人電腦基本上爲具有開放構造之系統之故，個人電腦之數位內容之保護實際上有其困難。此係由於在個人電腦上雖然數位內容係以檔案形式被處理，但是檔案之複製／移動基板上可以自由進行之故也。特別是關於被當成個人電腦之儲存裝置使用之硬碟機，其之規格係開放式，謀求被記錄於硬碟機上之數位內容之祕密化很困難。因此，由網際網路下載之數位內容一旦記錄在硬碟機後，可以將該數位內容由硬碟機自由地複製於其它之媒體使用。

發明摘要

因此，本發明之目的在於提供：即使在硬碟機之類的開放式記憶媒體中記錄內容之情形，可以保護該內容被不正當使用，能一併謀求數位內容之利用與保護之電腦系統

五、發明說明（2）

及內容保護方法。

依據本發明之一觀點，提供一種在記錄媒體可以記錄內容之電腦系統，其特徵係包含：爲了應記錄於前述記錄媒體之內容管理，記憶對應前述記憶媒體之ＩＤ之ＩＤ記憶手段，該ＩＤ記憶手段係有別於前述記錄媒體而設置；及在前述記錄媒體記錄內容之時，藉由前述ＩＤ記憶手段使用對應前述記憶媒體之ＩＤ，實施記錄前述內容之加密之內容管理手段。

依據本發明之其它觀點，提供一種在記錄媒體可以記錄內容之電腦系統，其特徵係包含：記憶限制被附加在前述內容之再生／複製／移動用之控制資訊，以及對應前述記錄媒體之ＩＤ之記憶手段，該ＩＤ記憶手段係有別於前述記錄媒體而設置；及在被記錄於前述記錄媒體之內容的再生、或對其它記錄媒體之複製或移動被要求時，依據前述控制資訊與前述ＩＤ，許可或禁止前述被要求之處理的實行之內容管理手段。

依據本發明之其它的觀點，係提供一種電腦系統，其特徵係包含：記憶被使用於內容之安全管理用之裝置ＩＤ之裝置ＩＤ記憶手段；及利用每個應記錄內容之記錄媒體中該記錄媒體所具有之裝置ＩＤ，可以管理前述內容之加密／解碼之內容管理手段，在不具有前述裝置ＩＤ之記錄媒體記錄內容之情形，使用前述裝置ＩＤ管理前述內容之加密／解碼之內容管理手段。

依據本發明之其它觀點，係提供一種電腦系統，其特

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（ 3 ）

徵係包含：記憶被使用於內容之安全管理用之裝置ＩＤ之裝置ＩＤ記憶手段；及利用每個應記錄內容之記錄媒體中該記錄媒體所具有之媒體ＩＤ，可以管理前述內容之加密／解碼之內容管理手段，在不具有前述媒體ＩＤ之記錄媒體記錄內容之情形，使用前述裝置ＩＤ管理前述內容之加密／解碼之內容管理手段，其中前述裝置ＩＤ記憶手段之裝置ＩＤ係藉由前述電腦系統之ＢＩＯＳ被管理，前述內容管理手段藉由與前述ＢＩＯＳ之認證由前述ＢＩＯＳ取得前述裝置ＩＤ，在前述內容被附加限制該內容之再生／複製／移動用之限制資訊，前述ＢＩＯＳ管理前述控制資訊之改變檢測用之編碼資料，前述內容管理手段在將被記錄於不具有前述媒體ＩＤ之內容複製於其它記錄媒體之情形，使前述內容之複製可能次數值減少１地更新不具有前述媒體ＩＤ之記錄媒體內之控制資訊，同時將被記錄於不具有前述媒體ＩＤ之記錄媒體之內容與前述更新後之控制資訊複製於前述其它之記錄媒體，而且依據更新後之控制資訊更新前述改變檢測用編碼資料之值。

依據本發明之進一步之其它的觀點，係提供一種可以處理內容之電腦系統，其特徵爲包含：進行前述內容之安全管理之內容管理手段，該內容管理手段包含：在具有媒體ＩＤ之記錄媒體記錄內容之情形，使用前述媒體ＩＤ加密前述內容或該內容之密碼鍵，記錄於具有前述媒體ＩＤ之記錄媒體之手段；及在不具有媒體ＩＤ之記錄媒體記錄內容之情形，使用藉由前述電腦系統之ＢＩＯＳ被管理之

五、發明說明（4）

前述電腦系統固有之裝置ＩＤ，加密前述內容或該內容之密碼鍵，記錄於不具有前述媒體ＩＤ之記錄媒體之手段。

依據本發明之其它的觀點，係提供一種電腦系統，其特徵爲包含：電腦系統之硬體控制用之系統程式，該系統程式管理前述電腦系統固有之裝置ＩＤ；及利用前述電腦系統固有之裝置ＩＤ，管理應記錄於前述電腦系統之記錄媒體之內容之加密／解碼之內容管理手段。

依據本發明之其它的觀點，係提供一種在電腦系統具有固有之裝置ＩＤ之電腦系統，其特徵爲包含：由前述電腦系統取得前述裝置ＩＤ，使用該取得之裝置ＩＤ，管理應記錄於前述電腦系統之記錄媒體之內容之加密／解碼之內容管理手段。

依據本發明之其它的觀點，係提供一種被適用於可以處理內容之電腦系統，保護前述內容被不正當使用之內容保護方法，其特徵爲：在具有媒體ＩＤ之記錄媒體記錄內容之情形，使用前述媒體Ｄ加密前述內容或該內容之密碼鍵，記錄於具有前述媒體ＩＤ之記錄媒體；及在不具有媒體ＩＤ之記錄媒體記錄內容之情形，使用藉由前述電腦系統內之ＢＩＯＳ被管理之前述電腦系統固有之裝置ＩＤ，加密前述內容或該內容之密碼鍵，記錄於不具有前述媒體ＩＤ之記錄媒體。

依據本發明之其它的觀點，係提供一種保護以具有系統固有之裝置ＩＤ之電腦系統被處理之內容被不正當使用之內容保護方法，其特徵爲：由前述電腦系統取得前述裝

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（ 5 ）

置ＩＤ；及使用前述取得之裝置ＩＤ，管理應記錄於前述電腦系統之記錄媒體之內容之加密／解碼。

依據本發明之其它的觀點，係提供一種保護在電腦系統被處理之內容被不正當使用之內容保護方法，其特徵爲：藉由前述電腦系統之硬體控制用之系統程式管理前述電腦系統固有之裝置ＩＤ，由前述系統程式取得前述裝置ＩＤ；及使用前述取得之裝置ＩＤ，管理應記錄於前述電腦系統之記錄媒體之內容之加密／解碼。

發明之詳細說明

以下，參考圖面說明本發明之實施形態。

圖１係顯示本發明之一實施形態之個人電腦之系統構成。此個人電腦（ＰＣ）１１爲可以處理影像資料或音樂資料等之各種數位內容之電腦系統。此個人電腦１１之內容保護方法係以：在每個應記錄內容之媒體利用該記錄媒體之媒體ＩＤ以管理內容之加密／解碼爲前提。此係如爲同一記錄媒體，爲了使之在其它個人電腦或電子機器使用也可以再生該記錄媒體之故，內容係使用被準備在各記錄媒體之專用的媒體ＩＤ以加密被記錄著。使用媒體ＩＤ之內容的加密／解碼之管理係藉由爲此之專用的軟體之安全管理者１１２被實行。此安全管理者１１２係以篡改．防止．軟體而被實現。所謂篡改．防止．軟體係意指：對於不正當之內部解析或篡改等之攻擊（attack）具備防衛機能之軟體。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（6）

安全管理者１１２係如圖示般地，位於應用程式１１１與檔案系統１１３之間，保護對向之內容之「記錄」、「再生」、「複製」、「移動」等之各種操作係透過安全管理者１１２進行。藉由安全管理者１１２之內容的加密／解碼管理可以大致區分爲：１）對於內藏專用之媒體ＩＤ之記錄媒體者，及２）對於不具有媒體ＩＤ之通常的記錄媒體者。

（具有媒體ＩＤ之記錄媒體）

首先，說明對於具有媒體ＩＤ之記錄媒體之處理。

記錄媒體（Ａ）１１６以及記錄媒體（Ｂ）１１７係分別對應安全管理者１１２之專用記錄媒體。這些記錄媒體可以使用可以安裝、拆下自如地裝置在個人電腦１１或其它之各種電子機器之記憶卡等之各種媒體（ＳＳＦＤＣ、快閃ＰＣ卡、迷你碟）等。

在記錄媒體（Ａ）１１６在通常之資料記憶領域之外，設置有：該記錄媒體固有之媒體ＩＤ（ＩＤＡ）被預先記憶之ＲＯＭ領域，以及儲存由後述之ＧＩ（Governance Information：管理資訊）表所製作之ＧＩ校驗和資料用之ＧＩ校驗和領域。記錄媒體（Ｂ）１１７也係同樣構成。媒體ＩＤ只要是各記錄媒體所固有即可，可以使用序列號碼或製造號碼、其它各樣之辨識資訊。

所謂ＧＩ表係對每一保護對象之各內容規定其之再生、複製、移動之可否、以及複數可能次數、移動可能次數

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（ 7 ）

等之複製控制資訊。ＧＩ校驗和資料係檢測ＧＩ表之內容之篡改用之改變檢測用編碼資料，由ＧＩ表之值被計算出。也可以使用ＧＩ表之雜碼（ hash ）值以代替ＧＩ校驗和資料。ＧＩ表之「複製可能次數」之值在複製每被實行時被減掉１。如此在ＧＩ表之值被更新之時，配合該更新，ＧＩ校驗和資料之值也被更新。因此，ＧＩ校驗和領域係由可以重寫之領域構成。

ＲＯＭ領域以及ＧＩ校驗和領域之任一種皆係使用者無法存取之安全領域。

在將內容記憶於記錄媒體（Ａ）１１６之情形，安全管理者１１２使用記錄媒體（Ａ）１１６之媒體ＩＤ管理內容之加密／解碼。在此情形，以下之資料被儲存在記錄媒體（Ａ）１１６之資料領域。

．Ｋｃ〔 Content 〕：藉由被稱爲內容Ｋｃ之密碼鍵被加密之內容

．ＧＩ

．ＩＤＡ〔Ｋｃ〕：藉由記錄媒體（Ａ）１１６之媒體ＩＤ（ＩＤＡ）被加密之內容鍵

在再生被記錄於記錄媒體（Ａ）１１６之內容之情形，安全管理者１１２首先使用記錄媒體（Ａ）１１６之媒體ＩＤ（ＩＤＡ），解碼ＩＤＡ〔Ｋｃ〕，獲得Ｋｃ。而且，藉由該Ｋｃ解碼Ｋｃ〔 Content 〕。

被記錄於記錄媒體（Ａ）１１６之內容如爲可以複製之內容之情形，可以將該內容由記錄媒體（Ａ）１１６複

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（8）

製於其它之記錄媒體（例如記錄媒體（Ｂ）１１７）。在此情形，安全管理者１１２由被儲存在記錄媒體（Ａ）１１６之ＧＩ產生校驗和，將該校驗和資料與記錄媒體（Ａ）１１６之ＧＩ校驗和領域之ＧＩ校驗和資料比較。在不一致之情形，複製被禁止。在一致之情形，安全管理者１１２使用記錄媒體（Ａ）１１６之媒體ＩＤ（ＩＤＡ）解碼ＩＤＡ〔Ｋｃ〕，獲得Ｋｃ。接著，安全管理者１１２使用複製目的地之記錄媒體（Ｂ）１１７之媒體ＩＤ（ＩＤＢ），加密Ｋｃ，將加密之內容鍵（ＩＤＢ〔Ｋｃ〕）與Ｋｃ〔Content〕以及ＧＩ一齊地寫入記錄媒體（Ｂ）１１７之資料領域。在此情形，記錄媒體（Ａ）１１６、記錄媒體（Ｂ）１１７之藉由ＧＩ被指定之可以複製次數之值都被減少１。例如，在複製之內容爲「只可複製一次」之內容之情形，被變更爲「無法再複製」之內容。又，伴隨ＧＩ之更新，記錄媒體（Ａ）１１６、記錄媒體（Ｂ）１１７之各別的ＧＩ校驗和之值也被更新。

被記錄於記錄媒體（Ａ）１１６之內容爲可以移動之內容之情形，可以將該內容由記錄媒體（Ａ）１１６移動於其它之記錄媒體（記錄媒體（Ｂ）１１７）。在此情形，安全管理者１１２由被儲存於記錄媒體（Ａ）１１６之ＧＩ產生校驗和資料，將該校驗和資料與記錄媒體（Ａ）１１６之ＧＩ校驗和領域之ＧＩ校驗和資料比較。在不一致之情形，移動被禁止。在一致之情形，安全管理者１１２使用記錄媒體（Ａ）１１６之媒體ＩＤ（ＩＤＡ）

五、發明說明（９）

，解碼ＩＤＡ〔Ｋｃ〕，獲得Ｋｃ。接著，安全管理者１１２使用移動目的地之記錄媒體（Ｂ）１１７之媒體ＩＤ（ＩＤＢ），加密Ｋｃ，將加密之內容鍵（ＩＤＢ〔Ｋｃ〕）與Ｋｃ〔Ｃｏｎｔｅｎｔ〕以及ＧＩ一齊地寫入記錄媒體（Ｂ）１１７之資料領域。之後，安全管理者１１２消除被儲存在移動源之記錄媒體（Ａ）１１６之資料領域之Ｋｃ〔Ｃｏｎｔｅｎｔ〕、ＧＩ、ＩＤＡ〔Ｋｃ〕，同時消除ＧＩ校驗和領域之ＧＩ校驗和資料。在藉由ＧＩ被規定者在只是「複製可能次數」而未規定「移動可能次數」之情形，不進行因移動之ＧＩ的更新。在「移動可能次數」被規定之情形，與前述之「複數」之情形相同，在ＧＩ被更新後，被寫入記錄媒體（Ｂ）１１７，又，對應該更新後之ＧＩ之校驗和資料變成被寫入ＧＩ校驗和領域。

（不具有媒體ＩＤ之記錄媒體）

接著，說明對於不具有媒體ＩＤ之處理。ＨＤＤ１１５係被當成個人電腦１１之二次記憶裝置使用之儲存裝置，被固定於個人電腦１１而使用。在ＨＤＤ１１５並沒有設置記錄媒體（Ａ）１１６以及記錄媒體（Ｂ）１１７之類的ＲＯＭ領域或ＧＩ校驗和領域。

使用ＨＤＤ１１５進行內容之記錄、複製、移動等之情形，安全管理者１１２使用本個人電腦１１所固有之裝置ＩＤ以代替媒體ＩＤ，進行內容之加密／解碼之管理。即安全管理者１１２在內容之記錄目的地、複製目的地、

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（10）

複製源、移動目的地或移動源爲對應ＨＤＤ１１５之驅動器號碼之情形，並非使用媒體ＩＤ而係使用在系統內被管理之裝置ＩＤ。在此情形，哪個驅動器號碼之記錄媒體具有媒體ＩＤ，哪個驅動器號碼之記錄媒體不具有媒體ＩＤ例如藉由利用隨插即用等之機能，可以使安全管理者１１２可以每個媒體都能辨識。

ＰＣ１１固有之裝置ＩＤ係藉由ＰＣ１１之硬體控制用之系統程式之ＢＩＯＳ被管理。在此ＢＩＯＳ之管理下，設置有：快閃ＢＩＯＳ－ＲＯＭ１４、鑲嵌式控制器（副ＣＰＵ）１２１以及快閃ＲＯＭ１２２。

快閃ＢＩＯＳ－ＲＯＭ１１４具有使用者無法存取之安全領域，在此如圖２所示般地，除了通行密碼區域之外，設置有ＩＤ區域、校驗和區域。通行密碼區域爲記憶依據使用者被登錄之通行密碼用之領域。在通行密碼被登錄之情形，判斷電源投入時由使用者輸入之通行密碼與登錄通行密碼之一致的有無，只在一致之情形，由ＯＳ之保護或暫停／睡眠狀態之回復變成可能。

ＰＣ１１固有之裝置ＩＤ（ＩＤＳ）被預先記憶在ＩＤ區域。校驗和區域係被使用於由被記憶在ＨＤＤ１１５之內容的ＧＩ產生ＧＩ校驗和資料之儲存。

另一方面，鑲嵌式控制器１２１相當於鍵盤控制器或電源控制器，在ＢＩＯＳ之控制下，可以存取快閃ＲＯＭ１２２。快閃ＲＯＭ１２２具有與快閃ＢＩＯＳ－ＲＯＭ１１４同樣之安全領域。

五、發明說明（11）

上述ＩＤＳ以及ＧＩ校驗和資料雖然被儲存在快閃ＢＩＯＳ－ＲＯＭ１１４與快閃ＲＯＭ１２２之中之任何一個的安全領域都可以，但是在本實施形態中，以利用快閃ＢＩＯＳ－ＲＯＭ１１４之安全領域爲例說明之。

在ＢＩＯＳ設置與安全管理者１１２之間進行認證處理用之認證機能。藉由安全管理者１１２與ＢＩＯＳ之認證處理一被確認互相彼此爲正確的程式，安全管理者１１２可以由ＢＩＯＳ取得裝置ＩＤ（ＩＤＳ）。如此，藉由與ＢＩＯＳ之認證第１次取得裝置ＩＤ，可以更安全地管理裝置ＩＤ。

接著，參考圖３以及圖５具體說明使用ＨＤＤ１１５之情形之內容管理處理之順序。

「記錄」

圖３係顯示內容記錄時之動作流程。

（步驟Ｓ１）：在ＰＣ１１之啓動時，首先在安全管理者１１２與ＢＩＯＳ之間實行認證處理。一被確認彼此爲互相正確之程式，在安全管理者１１２與ＢＩＯＳ之間進行鍵交換，同一之認證鍵（Ｋｘ２）被共有。認證鍵（Ｋｘ２）係每次改變之時變鍵。

（步驟Ｓ２）：安全管理者１１２對ＢＩＯＳ發行ＩＤ取得要求。響應由安全管理者１１２之ＩＤ取得要求，ＢＩＯＳ將裝置ＩＤ（ＩＤＳ）以認證鍵（Ｋｘ２）加密，將被加密之裝置ＩＤ（Ｋｘ２〔ＩＤＳ〕）發送於安

五、發明說明（12）

全管理者１１２。安全管理者１１２保持認證鍵（Ｋｘ２）之故，可以由Ｋｘ２〔ＩＤＳ〕解讀ＩＤＳ。

（步驟Ｓ３）：在使用ＷＥＢ瀏覽器等之應用程式由ＷＥＢ伺服器下載影像資料或音樂資料等之內容之情形，透過ＷＥＢ瀏覽器或直接在安全管理者１１２與ＷＥＢ伺服器１２間進行認證處理。一被確認爲彼此互相具有正確內容保護機能者，在安全管理者１１２與ＷＥＢ伺服器１２之間進行鍵交換，同一之認證鍵（Ｋｘ１）被共有。認證鍵（Ｋｘ１）係每次改變之時變鍵。

（步驟Ｓ４）：ＷＥＢ伺服器１２將被要求之內容以規定之內容鍵Ｋｃ加密之（Ｋｃ〔Content〕）以及以認證鍵（Ｋｘ１）加密之內容鍵（Ｋｘ１〔Ｋｃ〕）以及ＧＩ發送於ＰＣ１１。

（步驟Ｓ５）：這些Ｋｃ〔Content〕、Ｋｘ１〔Ｋｃ〕、ＧＩ透過ＷＥＢ瀏覽器等被送往安全管理者１１２。安全管理者１１２在由ＷＥＢ瀏覽器指定之下載目的地之記錄媒體爲ＨＤＤ１１５之情形，使用認證鍵（Ｋｘ１）與由ＢＩＯＳ取得之裝置ＩＤ（ＩＤＳ），將Ｋｘ１〔Ｋｃ〕轉換爲ＩＤＳ〔Ｋｃ〕。在此情形，首先，使用認證鍵（Ｋｘ１），Ｋｘ１〔Ｋｃ〕被解碼爲Ｋｃ，該Ｋｃ重新藉由ＩＤＳ被加密。

之後，安全管理者１１２將Ｋｃ〔Content〕、ＩＤＳ〔Ｋｃ〕、ＧＩ通過檔案系統１１３，進而ＩＤＥ驅動器等，寫入ＨＤＤ１１５。

五、發明說明（13）

（步驟Ｓ６）：安全管理者１１２由ＧＩ算出ＧＩ校驗和資料（ＧＩ＿ＣＳ），將其以與ＢＩＯＳ之認證鍵（Ｋｘ２）加密，傳達於ＢＩＯＳ。ＢＩＯＳ將ＧＩ校驗和資料於被加密下或解碼後，寫入快閃ＢＩＯＳ－ＲＯＭ１１４之校驗和區域。當然安全管理者１１２將ＧＩ校驗和資料或其之加密資料直接寫入快閃ＢＩＯＳ－ＲＯＭ１１４之校驗和區域也可以。

「再生」

圖４係顯示內容再生時之動作流程。

（步驟Ｔ１）：在ＰＣ１１之啓動時，首先在安全管理者１１２與ＢＩＯＳ之間實行認證處理。一被確認彼此互相爲正確程式，在安全管理者１１２與ＢＩＯＳ之間進行鍵交換處理，同一之認證鍵（此處設爲Ｋｘ１）被共有。認證鍵（Ｋｘ１）爲每次改變之時變鍵。

（步驟Ｔ２）：響應由安全管理者１１２之ＩＤ取得要求，ＢＩＯＳ將裝置ＩＤ（ＩＤＳ）以認證鍵（Ｋｘ２）加密，將被加密之裝置ＩＤ（Ｋｘ１〔ＩＤＳ〕）發送於安全管理者１１２。安全管理者１１２保持認證鍵（Ｋｘ１）之故，可以由Ｋｘ１〔ＩＤＳ〕解讀ＩＤＳ。

（步驟Ｔ３）：接著，響應安全管理者１１２來之ＧＩ校驗和資料之取得要求，ＢＩＯＳ以認證鍵（Ｋｘ１）加密ＧＩ校驗和資料（ＧＩ＿ＣＳ），將被加密之ＧＩ校驗和資料（Ｋｘ１〔ＧＩ＿ＣＳ〕）發送於安全管理者

五、發明說明（14）

112。安全管理者112保持認證鍵（Kx1）之故，可以由Kx1〔GI－CS〕解讀GI－CS。

（步驟T4）：安全管理者112透過檔案系統113，進而IDE驅動器等由HDD115取得由應用程式111等被指定之再生對象之被加密之內容（（Kc〔Content〕））以及與其對應之IDS〔Kc〕以及GI。

（步驟T5）：安全管理者112由GI算出校驗和，將該算出之校驗和與由BIOS取得之GI－CS比較。在不一致之情形，有HDD115之GI藉由具惡意之使用者被重寫之虞之故，再生處理在此時終止。在一致之情形，安全管理者112使用由BIOS取得之IDS，解碼IDS〔Kc〕，獲得Kc。而且使用該Kc解除Kc〔Content〕之密碼，將未加工之內容（Content）送往再生軟體（再生裝置）。再生軟體也以篡改．防止．軟體而被實現。

「複製」

圖5係顯示內容複製時之動作流程。此處例示將被記錄於HDD115之內容複製於記錄媒體（A）116之情形。

（步驟U1）：在PC11之啓動時，首先在安全管理者112與BIOS之間實行認證處理。一被確認彼此互相爲正確程式，在安全管理者112與BIOS之間進

五、發明說明（15）

行鍵交換處理，同一之認證鍵（此處設爲Ｋｘ１）被共有。認證鍵（Ｋｘ１）爲每次改變之時變鍵。

（步驟Ｕ２）：響應由安全管理者１１２之ＩＤ取得要求，ＢＩＯＳ將裝置ＩＤ（ＩＤＳ）以認證鍵（Ｋｘ２）加密，將被加密之裝置ＩＤ（Ｋｘ１〔ＩＤＳ〕）發送於安全管理者１１２。安全管理者１１２保持認證鍵（Ｋｘ１）之故，可以由Ｋｘ１〔ＩＤＳ〕解讀ＩＤＳ。

（步驟Ｕ３）：接著，響應安全管理者１１２來之ＧＩ校驗和資料之取得要求，ＢＩＯＳ以認證鍵（Ｋｘ１）加密ＧＩ校驗和資料（ＧＩ＿ＣＳ），將被加密之ＧＩ校驗和資料（Ｋｘ１〔ＧＩ＿ＣＳ〕）發送於安全管理者１１２。安全管理者１１２保持認證鍵（Ｋｘ１）之故，可以由Ｋｘ１〔ＧＩ－ＣＳ〕解讀ＧＩ－ＣＳ。

（步驟Ｕ４）：安全管理者１１２透過檔案系統１１３，進而ＩＤＥ驅動器等由ＨＤＤ１１５取得由應用程式１１１等被指定之複製對象之被加密之內容（（Ｋｃ〔Content〕））以及與其對應之ＩＤＳ〔Ｋｃ〕以及ＧＩ。

安全管理者１１２由ＧＩ算出校驗和，將該算出之校驗和與由ＢＩＯＳ取得之ＧＩ－ＣＳ比較。在不一致之情形，有ＨＤＤ１１５之ＧＩ藉由具惡意之使用者被重寫之虞之故，複製處理在此時終止。在一致之情形，參考ＨＤＤ１１５之ＧＩ，調查複製對象之內容是否爲可以複製之內容。在「不可複製」或「複製可能次數＝零」之情

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（16）

形，複製處理在此時終止。如係可被複製之內容，安全管理者１１２進入下述之步驟Ｕ５以後之處理。

（步驟Ｕ５）：安全管理者１１２進行與複製目的地之記錄媒體（Ａ）１１６或控制其之裝置驅動器之間之認證處理。一被確認彼此互相具有正確內容保護機能，在安全管理者１１２與複製目的地之記錄媒體（Ａ）１１６或其之裝置驅動器之間進行鍵交換，同一之認證鍵（此處設爲Ｋｘ２）被共有。認證鍵（Ｋｘ２）爲每次改變之時變鍵。

（步驟Ｕ６）：響應由安全管理者１１２之ＩＤ取得要求，記錄媒體（Ａ）１１６或其之裝置驅動器以認證鍵（Ｋｘ２）加密媒體ＩＤ（ＩＤＡ），將被加密之媒體ＩＤ（Ｋｘ２〔ＩＤＡ〕）發送於安全管理者１１２。安全管理者１１２保持認證鍵（Ｋｘ２）之故，可以由Ｋｘ２〔ＩＤＡ〕解讀ＩＤＡ。

（步驟Ｕ７）：安全管理者１１２更新由ＨＤＤ１１５取得之ＧＩ，獲得「複製可能次數」被減１之ＧＩ´。而且，使用由ＢＩＯＳ取得之裝置ＩＤ（ＩＤＳ），解碼ＩＤＳ〔Ｋｃ〕，獲得Ｋｃ。接著，安全管理者１１２使用媒體ＩＤＡ加密Ｋｃ，獲得ＩＤＡ〔Ｋｃ〕。之後，安全管理者１１２將Ｋｃ〔Content〕、ＩＤＡ〔Ｋｃ〕、ＧＩ´透過檔案系統１１３進而記錄媒體（Ａ）１１６之驅動器等寫入記錄媒體（Ａ）１１６。

（步驟Ｕ８）：安全管理者１１２算出由ＧＩ´之校

五、發明說明（17）

驗和資料（ＧＩ´＿ＣＳ），將其以認證鍵（Ｋｘ２）加密者（Ｋｘ２〔ＧＩ´＿ＣＳ〕）發送於記錄媒體（Ａ）１１６或其之驅動器，將ＧＩ´＿ＣＳ寫入記錄媒體（Ａ）１１６之ＧＩ校驗和資料領域。

（步驟Ｕ９）：之後，安全管理者１１２將校驗和資料（ＧＩ´＿ＣＳ），以與ＢＩＯＳ之認證鍵（Ｋｘ１）加密，將其傳達於ＢＩＯＳ。ＢＩＯＳ將快閃ＢＩＯＳ－ＲＯＭ１１４之校驗和區域之內容重寫於ＧＩ´＿ＣＳ。

（步驟Ｕ１０）：而且，安全管理者１１２將ＨＤＤ１１５之ＧＩ更新爲ＧＩ´。

「移動」

在將被記錄於ＨＤＤ１１５之內容移動於記錄媒體（Ａ）１１６之情形，與圖５之複製處理基本上雖係以相同順序進行，但是與複製處理不同之點爲：取代步驟Ｕ９，進行消除快閃ＢＩＯＳ－ＲＯＭ１１４之校驗和區域之內容之處理，又，取代圖５之步驟Ｕ１０，進行消除ＨＤＤ１１５之Ｋｃ〔Content〕、ＩＤＳ〔Ｋｃ〕、以及ＧＩ之處理。又，移動之情形，不進行對於複製可能次數之ＧＩ的更新，除了移動可能次數被規定之情形，ＧＩ不被更新地被寫入移動目的地之記錄媒體（Ａ）１１６。

如上述般地，本實施形態中，藉由使ＢＩＯＳ具有與安全管理者１１２之認證機能或裝置ＩＤ管理機能，即使在不具有裝置ＩＤ之記錄媒體記錄內容之情形，與使用具

五、發明說明（ 18）

有媒體ＩＤ之專用的記錄媒體之情形相同地，可以謀求被記錄於其上之內容之保護。

特別是藉由ＢＩＯＳ管理裝置ＩＤ以及ＧＩ校驗和資料，使無法由系統側存取之故，對於ＨＤＤ１１５不用加上任何變更，可以保護下載於ＨＤＤ１１５之內容被不正當使用。

又，在本實施形態中，雖然使用媒體ＩＤ或裝置ＩＤ加密內容之密碼鍵之內容鍵，但是也可以將媒體ＩＤ或裝置ＩＤ當成內容鍵使用，使用媒體ＩＤ或裝置ＩＤ加密內容本身。

又，在本實施形態中，雖然以ＨＤＤ爲不具有媒體ＩＤ之記憶媒體爲例，但是使用裝置ＩＤ以進行加密／解碼之管理之本實施形態之內容保護方法例如對於ＭＯ或記憶卡（ＰＣ卡獲緻密快閃記憶卡等）或智慧媒體等不具有媒體ＩＤ之通常的不揮發性記憶媒體全體都可以適用。

又，裝置ＩＤ可以記憶於ＰＣ１１內之安全的記憶裝置，例如也可以記憶於ＰＣ１１內之埋入控制器（ＥＣ）內，被設置在ＰＣ１１內之即時時脈內之以電池備援之ＣＭＯＳ之記憶體等。即使在ＰＣ１１內之任何地方記憶裝置ＩＤ之情形，藉由透過ＢＩＯＳ取得裝置ＩＤ，安全管理者１１２可以不意識裝置ＩＤ之記憶場所進行必要之處理。

再者，本實施形態不限於ＰＣ，也可以適用於機上盒（ setup box ）、遊戲機、音頻／錄像機等、搭載微處理器

五、發明說明（19）

之所有的資料處理裝置（電腦應用機器）。

又，安全管理者１１２之機能，即藉由將包含：如前述般地由ＢＩＯＳ取得裝置ＩＤ，使用該裝置ＩＤ管理內容之加密／解碼之順序，或具有媒體ＩＤ之記錄媒體使用該媒體ＩＤ管理內容之加密／解碼之順序等之電腦程式透過通訊媒體或記錄媒體導入電腦，藉由ＢＩＯＳ可以管理裝置ＩＤ之系統，可以獲得與本實施形態相同之效果。

又，ＢＩＯＳ也是可以更新之故，在通常之硬體控制機能之外，如將具有裝置ＩＤ以及其之管理機能等之新的ＢＩＯＳ透過通訊媒體或記錄媒體導入電腦，即使在既存之電腦也可以獲得與本實施形態相同之效果。

如以上詳細敘述般地，依據本發明，即使在硬碟機之類的開放式記錄媒體記錄內容之情形，可以保護該內容被不正當使用，可以一併謀求數位內容之利用與保護。

圖面之簡單說明

圖１係顯示本發明之一實施形態之電腦系統之基本構成方塊圖。

圖２係顯示被設於同一實施形態之電腦系統之快閃ＢＩＯＳ＿ＲＯＭ之記憶內容之一例圖。

圖３係顯示在同一實施形態之電腦系統所進行之內容記錄處理之順序圖。

圖４係顯示在同一實施形態之電腦系統所進行之再生處理之順序圖。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（ 20）

圖 5 係顯示在同一實施形態之電腦系統所進行之內容複製之順序圖。

主要元件對照表

10	網際網路
12	WEB伺服器
111	應用程式
112	安全管理者
113	檔案系統
116	記錄媒體A
117	記錄媒體B

六、申請專利範圍

1．一種電腦系統，係在記錄媒體可以記錄內容之電腦系統，其特徵爲具備：

爲了應記錄於前述記錄媒體之內容管理，記憶對應前述記憶媒體之ＩＤ之ＩＤ記憶手段（１１４或１２２），該ＩＤ記憶手段（１１４或１２２）係有別於前述記錄媒體而設置；

及在前述記錄媒體記錄內容之時，藉由前述ＩＤ記憶手段（１１４或１２２）使用對應前述記憶媒體之ＩＤ，實施記錄前述內容之加密之內容管理手段（１１２）。

2．如申請專利範圍第1項記載之電腦系統，其中上述ＩＤ記憶手段（１１４或１２２）之ＩＤ係藉由前述電腦系統之ＢＩＯＳ所管理，

前述內容管理手段（１１２）係藉由與前述ＢＩＯＳ之認證由前述ＢＩＯＳ取得前述ＩＤ。

3．如申請專利範圍第2項記載之電腦系統，其中前述ＩＤ記憶手段（１１４或１２２）係由儲存前述ＢＩＯＳ用之ＢＩＯＳ－ＲＯＭ所構成，

前述ＢＩＯＳ－ＲＯＭ具有使用者無法存取之安全領域，前述ＩＤ被儲存在該領域。

4．一種電腦系統，其係可以在記錄媒體記憶內容之電腦系統，其特徵爲包含：

記憶限制被附加在前述內容之再生／複製／移動用之控制資訊，以及對應前述記錄媒體之ＩＤ之記憶手段（１１４或１２２），該記憶手段（１１４或１２２）係有

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

六、申請專利範圍

別於前述記錄媒體而設置；

及在被記錄於前述記錄媒體之內容的再生、或對其它記錄媒體之複製或移動被要求時，依據前述控制資訊與前述ＩＤ，許可或禁止前述被要求之處理的實行之內容管理手段（１１２）。

５．如申請專利範圍第４項記載之電腦系統，其中前述內容管理手段（１１２）在將被記錄於不具有前述ＩＤ之記錄媒體（１１５）之內容移動於其它記錄媒體之情形，將被記錄於不具有前述ＩＤ之記錄媒體（１１５）之控制資訊以及內容移動於前述其它之記錄媒體後，消除被記錄在不具有前述ＩＤ之記錄媒體（１１５）之內容以及控制資訊。

６．如申請專利範圍第５項記載之電腦系統，其中前述內容管理手段（１１２）在對於被記錄於不具有前述ＩＤ之記錄媒體（１１５）之內容，被要求對其它之記錄媒體之複製、或對其它的記錄媒體之移動時，使用前述ＩＤ解除前述內容或其之密碼鍵之加密後，使用複製目的地或移動目的地之其它的記錄媒體之ＩＤ，再度加密前述內容或其之內容的密碼鍵，記錄於前述其它之記錄媒體。

７．一種電腦系統，其特徵爲包含：

記憶被使用於內容之安全管理用之裝置ＩＤ（ＩＤＳ）之裝置ＩＤ記憶手段（１１４或１２２）；

及利用每個應記錄內容之記錄媒體中該記錄媒體所具有之裝置ＩＤ，可以管理前述內容之加密／解碼之內容管

六、申請專利範圍

理手段（１１２），在不具有前述裝置ＩＤ之記錄媒體記錄內容之情形，使用前述裝置ＩＤ（ＩＤＳ）管理前述內容之加密／解碼之內容管理手段。

８．如申請專利範圍第７項記載之電腦系統，其中上述裝置ＩＤ記憶手段（１１４或１２２）之裝置ＩＤ係藉由前述電腦系統之ＢＩＯＳ所管理，

前述內容管理手段（１１２）係藉由與前述ＢＩＯＳ之認證由前述ＢＩＯＳ取得前述裝置ＩＤ（ＩＤＳ）。

９．如申請專利範圍第８項記載之電腦系統，其中前述裝置ＩＤ記憶手段（１１４或１２２）係由儲存前述ＢＩＯＳ用之ＢＩＯＳ－ＲＯＭ所構成，

前述ＢＩＯＳ－ＲＯＭ具有使用者無法存取之安全領域，前述裝置ＩＤ（ＩＤＳ）被儲存在該領域。

１０．如申請專利範圍第８項記載之電腦系統，其中在前述內容被附加限制該內容之再生／複製／移動用之限制資訊，

前述內容管理手段（１１２）在被要求被記錄於不具有前述媒體ＩＤ之記錄媒體（１１５）之內容之再生、對其它記錄媒體之複製、或對其它記錄媒體之移動時，依據前述控制資訊與前述改變檢測用編碼資料，許可或禁止前述被要求之處理的實行。

１１．如申請專利範圍第１０項記載之電腦系統，其中前述內容管理手段（１１２）在將被記錄於不具有前述ＩＤ之記錄媒體（１１５）之內容移動於其它記錄媒體之

六、申請專利範圍

情形，將被記錄於不具有前述ＩＤ之記錄媒體（１１５）之控制資訊以及內容移動於前述其它之記錄媒體後，消除被記錄在不具有前述ＩＤ之記錄媒體（１１５）之內容以及控制資訊。

１２．如申請專利範圍第１１項記載之電腦系統，其中前述內容管理手段（１１２）在對於被記錄於不具有前述媒體ＩＤ之記錄媒體（１１５）之內容，被要求對其它之記錄媒體之複製、或對其它的記錄媒體之移動時，使用前述裝置ＩＤ（ＩＤＳ）解除前述內容或其之密碼鍵之加密後，使用複製目的地或移動目的地之其它的記錄媒體之媒體ＩＤ，再度加密前述內容或其之內容的密碼鍵，記錄於前述其它之記錄媒體。

１３．一種電腦系統，其特徵爲包含：

記憶被使用於內容之安全管理用之裝置ＩＤ（ＩＤＳ）之裝置ＩＤ記憶手段（１１４或１２２）；

及利用每個應記錄內容之記錄媒體中該記錄媒體所具有之裝置ＩＤ，可以管理前述內容之加密／解碼之內容管理手段（１１２），在不具有前述媒體ＩＤ之記錄媒體（１１５）記錄內容之情形，使用前述裝置ＩＤ（ＩＤＳ）管理前述內容之加密／解碼之內容管理手段（１１２）；

其中前述裝置ＩＤ記憶手段之裝置ＩＤ係藉由前述電腦系統之ＢＩＯＳ被管理，前述內容管理手段藉由與前述ＢＩＯＳ之認證由前述ＢＩＯＳ取得前述裝置ＩＤ，在前述內容被附加限制該內容之再生／複製／移動用之限制資

六、申請專利範圍

訊，前述ＢＩＯＳ管理前述控制資訊之改變檢測用之編碼資料，前述內容管理手段在將被記錄於不具有前述媒體ＩＤ之內容複製於其它記錄媒體之情形，使前述內容之複製可能次數值減少１地更新不具有前述媒體ＩＤ之記錄媒體內之控制資訊，同時將被記錄於不具有前述媒體ＩＤ之記錄媒體之內容與前述更新後之控制資訊複製於前述其它之記錄媒體，而且依據更新後之控制資訊更新前述改變檢測用編碼資料之值。

１４．如申請專利範圍第１３項記載之電腦系統，其中前述內容管理手段（１１２）在對於被記錄於不具有前述媒體ＩＤ之記錄媒體（１１５）之內容，被要求對其它之記錄媒體之複製、或對其它的記錄媒體之移動時，使用前述裝置ＩＤ（ＩＤＳ）解除前述內容或其之密碼鍵之加密後，使用複製目的地或移動目的地之其它的記錄媒體之媒體ＩＤ，再度加密前述內容或其之內容的密碼鍵，記錄於前述其它之記錄媒體。

１５．一種電腦系統，係一種可以處理內容之電腦系統，其特徵爲包含：

進行前述內容之安全管理之內容管理手段（１１２），該內容管理手段（１１２）包含：

在具有媒體ＩＤ之記錄媒體（１１６，１１７）記錄內容之情形，使用前述媒體ＩＤ加密前述內容或該內容之密碼鍵，記錄於具有前述媒體ＩＤ之記錄媒體之手段；

及在不具有媒體ＩＤ之記錄媒體（１１５）記錄內容

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

六、申請專利範圍

之情形，使用藉由前述電腦系統之ＢＩＯＳ被管理之前述電腦系統固有之裝置ＩＤ（ＩＤＳ），加密前述內容或該內容之密碼鍵，記錄於不具有前述媒體ＩＤ之記錄媒體（１１５）之手段。

１６．一種電腦系統，其特徵爲具有：

電腦系統之硬體控制用之系統程式，該系統程式管理前述電腦系統固有之裝置ＩＤ（ＩＤＳ）；

及利用前述電腦系統固有之裝置ＩＤ（ＩＤＳ），管理應記錄於前述電腦系統之記錄媒體之內容之加密／解碼之內容管理手段（１１２）。

１７．如申請專利範圍第１６項記載之電腦系統，其中在前述內容被附加限制該內容之再生／複製／移動用之限制資訊，

前述系統程式管理前述控制資訊之改變檢測用之編碼資料，

前述內容管理手段（１１２）在被要求被記錄於前述媒體之內容之再生、對其它記錄媒體之複製、或對其它記錄媒體之移動時，依據前述控制資訊與前述改變檢測用編碼資料，許可或禁止前述被要求之處理的實行。

１８．一種電腦系統，其係具有電腦系統所固有之裝置ＩＤ（ＩＤＳ）之電腦系統，其特徵爲包含：

由前述電腦系統取得前述裝置ＩＤ（ＩＤＳ），使用該取得之裝置ＩＤ（ＩＤＳ）管理應記錄於前述電腦系統之記錄媒體之內容的加密／解碼之內容管理手段（１１２

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

六、申請專利範圍

）。

１９．一種內容之保護方法，係提供一種被適用於可以處理內容之電腦系統，保護前述內容被不正當使用之內容保護方法，其特徵爲：

在具有媒體ＩＤ之記錄媒體（１１６，１１７）記錄內容之情形，使用前述媒體ＩＤ加密前述內容或該內容之密碼鍵，記錄於具有前述媒體ＩＤ之記錄媒體（１１６，１１７）；

及在不具有媒體ＩＤ之記錄媒體（１１５）記錄內容之情形，使用藉由前述電腦系統內之ＢＩＯＳ被管理之前述電腦系統固有之裝置ＩＤ（ＩＤＳ），加密前述內容或該內容之密碼鍵，記錄於不具有前述媒體ＩＤ之記錄媒體（１１５）。

２０．一種內容保護方法，其係一種保護以具有系統固有之裝置ＩＤ（ＩＤＳ）之電腦系統被處理之內容被不正當使用之內容保護方法，其特徵爲：

由前述電腦系統取得前述裝置ＩＤ（ＩＤＳ）；

及使用前述取得之裝置ＩＤ（ＩＤＳ），管理應記錄於前述電腦系統之記錄媒體之內容之加密／解碼。

２１．一種內容保護方法，其係一種保護在電腦系統被處理之內容被不正當使用之內容保護方法，其特徵爲：

藉由前述電腦系統之硬體控制用之系統程式管理前述電腦系統固有之裝置ＩＤ（ＩＤＳ）；

由前述系統程式取得前述裝置ＩＤ（ＩＤＳ）；

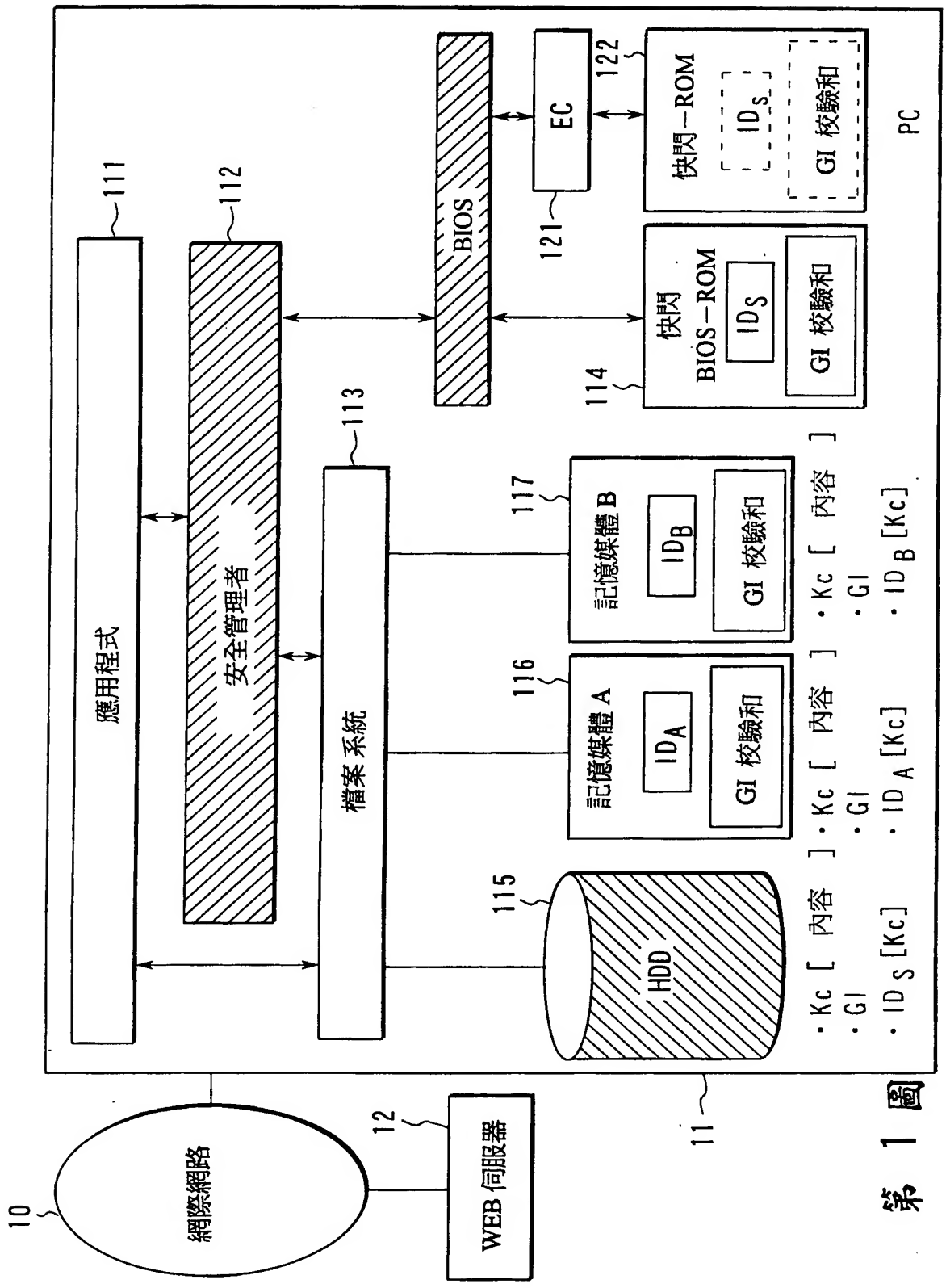
（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

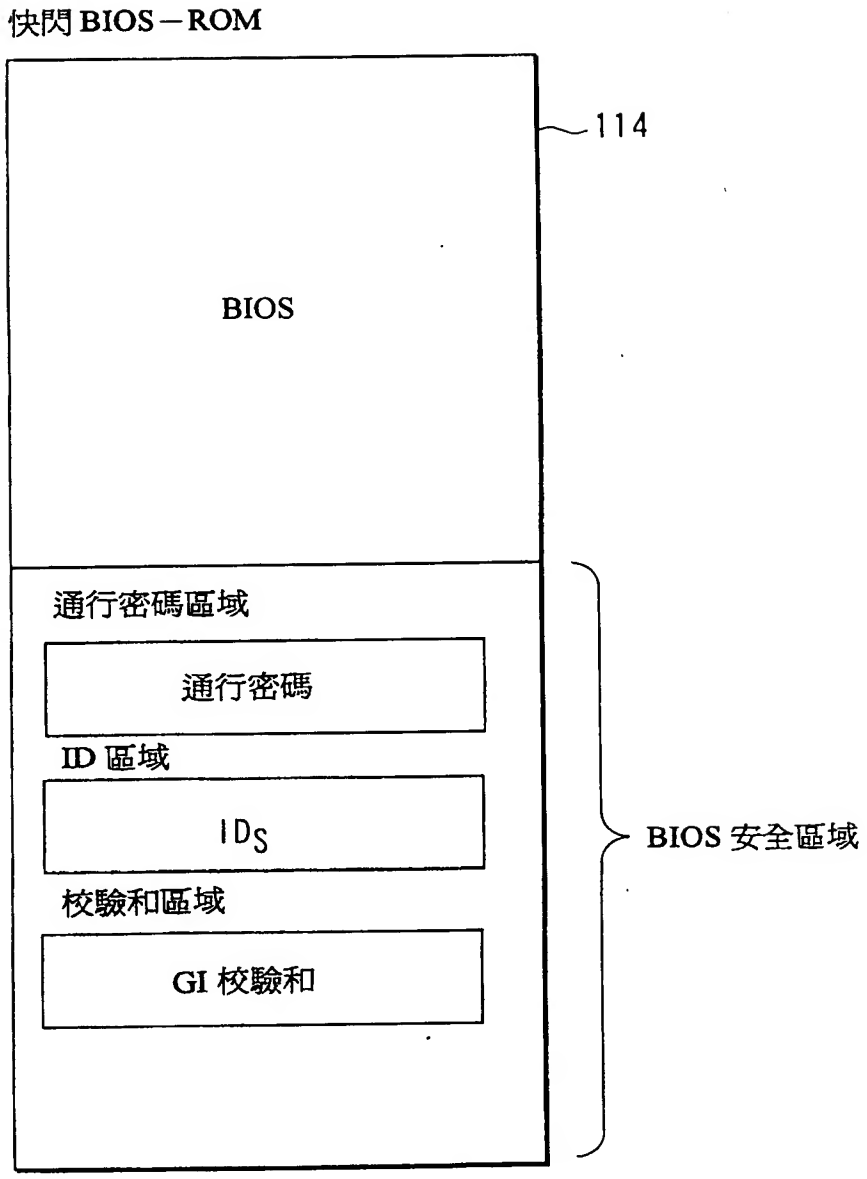
A8
B8
C8
D8

六、申請專利範圍

及使用前述取得之裝置ＩＤ（ＩＤＳ），管理應記錄於前述電腦系統之記錄媒體之內容之加密／解碼。

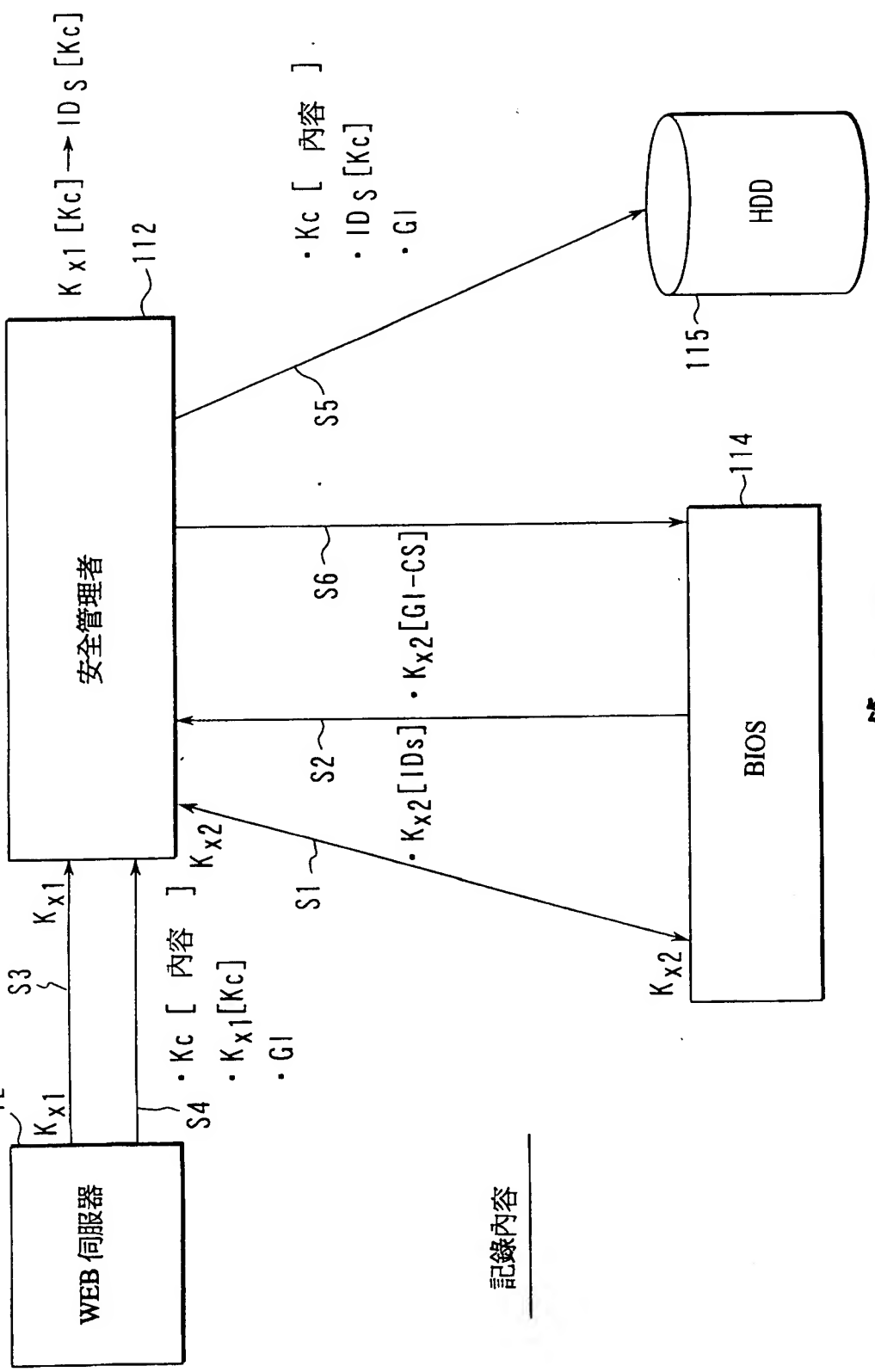

10
網際網路
12
WEB 伺服器
11
PC
111
應用程式
112
安全管理者
113
檔案 系統
115
HDD
・Kc [內容]
・GI
・ID S [Kc]
116
記憶媒體 A
ID A
GI 校驗和
・Kc [內容]
・GI
・ID A [Kc]
117
記憶媒體 B
ID B
GI 校驗和
・Kc [內容]
・GI
・ID B [Kc]
BIOS
121
EC
122
快閃－ROM
ID S
GI 校驗和
114
快閃 BIOS－ROM
ID S
GI 校驗和

第 1 圖


快閃 BIOS－ROM
114
BIOS
通行密碼區域
通行密碼
ID 區域
IDS
校驗和區域
GI 校驗和
BIOS 安全區域

第 2 圖

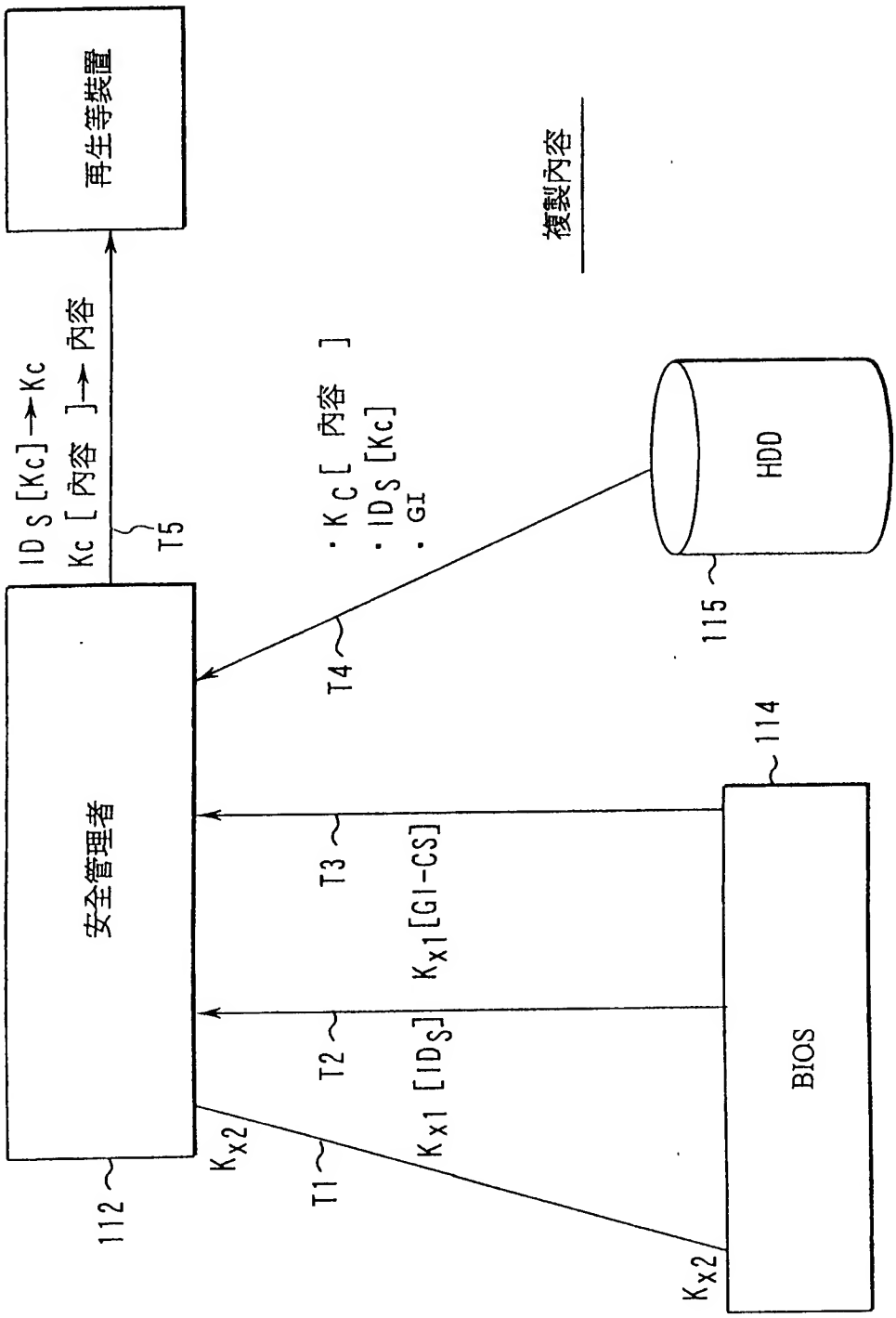
89104427



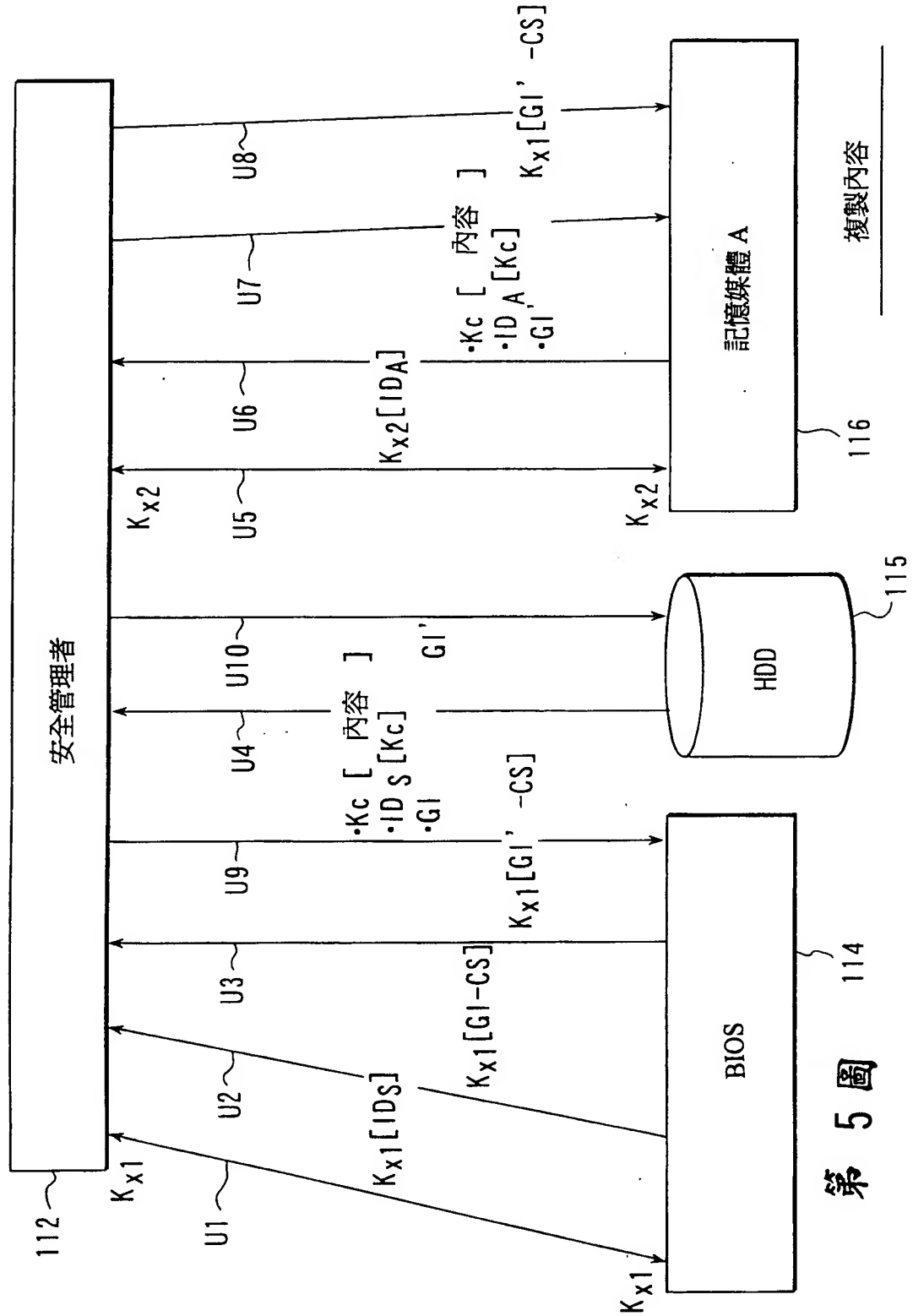
第 3 圖

附件 2: 第 89104427 號專利申請案
中文圖式修正頁 民國 90 年 11 月呈

90年11月2日 修正 補充



第 4 圖


安全管理者
112
K_{x1}
U1
$K_{x1}[IDS]$
U2
$K_{x1}[G1-CS]$
U3
·Kc [內容]
·ID S [Kc]
·G1
U4
$K_{x1}[G1'-CS]$
U9
G1'
U10
K_{x2}
U5
$K_{x2}[IDA]$
U6
·Kc [內容]
·ID A [Kc]
·G1'
U7
$K_{x1}[G1'-CS]$
U8
BIOS
114
HDD
115
記憶媒體 A
116
複製內容

第 5 圖